PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-030242
(43)Date of publication of application : 03.02.1992

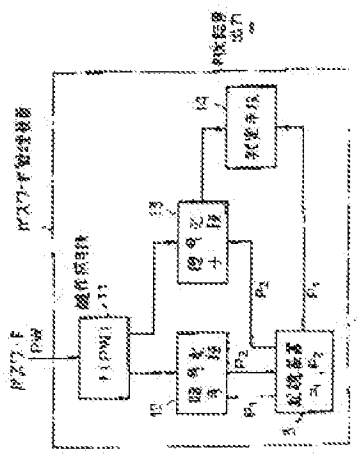
(51)Int.Cl. G06F 15/00

(21)Application number : 02-136866
(22)Date of filing : 25.05.1990

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KOBAYASHI TETSUJI

(54) PASSWORD CONTROL DEVICE

(57)Abstract:
PURPOSE: To safely control a password and to facilitate the control of a key by ciphering first open information through the use of the key, generating second public information, decoding second public information through the use of the key generated by the password checking whether the information coincides with first public information or not.
CONSTITUTION: A key generation means 11 generates the key from the password for registration PW, and a ciphering means 12 ciphers first public information by using the key. Then, second public information is generated and second public information and first public information are stored in a storage device 3. When the password PW is inputted, the key generation means 11 generates the key from the password, and a decoding means 13 decodes second open information by using the key. It is checked whether decoded information coincides with first public information, and a judgement means 14 judges that the inputted password is normal when they coincide. Thus, the password is safely controlled and the control of the key becomes easy.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－30242

⑤Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成4年(1992)2月3日
G 06 F 15/00	330 E	7218－5L	

審査請求　未請求　請求項の数 2　（全6頁）

⑭発明の名称　パスワード管理装置

⑳特　願　平2－136866

㉒出　願　平2(1990)5月25日

㉑発明者　小林　哲二　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

㉑出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

㉔代理人　弁理士　草野　卓

明　細　書

1.発明の名称

パスワード管理装置

2.特許請求の範囲

(1)　パスワードから鍵を作成する鍵作成手段と、

登録用パスワードについて上記鍵作成手段により作られた鍵を用いて第1公開情報を暗号化して第2公開情報を作成する暗号化手段と、

上記第1公開情報及び上記第2公開情報を記憶する記憶装置と、

入力されたパスワードについて、上記鍵作成手段により作られた鍵を用いて上記第2公開情報を復号化する復号化手段と、

その復号化された情報と上記第1公開情報とが一致するか否かを検査し、一致した時に上記入力されたパスワードを正常と判定する判定手段と、

を具備するパスワード管理装置。

(2)　登録用パスワードを鍵として第1公開情報を暗号化して第2公開情報を作成する暗号化手段と、

上記第1公開情報及び上記第2公開情報を記憶する記憶装置と、

入力されたパスワードを鍵として上記第2公開情報を復号化する復号化手段と、

その復号化された情報と上記第1公開情報とが一致するか否かを検査し、一致した時に上記入力されたパスワードを正常と判定する判定手段と、

を具備するパスワード管理装置。

3.発明の詳細な説明

〔産業上の利用分野〕

情報処理装置に対してアクセスする利用者の正当性を認証するために、パスワード（暗証番号と呼ばれることがある）が広く用いられている。

この発明は、情報処理装置で入力されたパスワードの正当性を検証するパスワード管理装置に関するものである。ここで情報処理装置とは、中央処理装置（CPU）及び記憶装置を有する装置であって（例えば、マイクロコンピュータ、パーソナルコンピュータ、ICカード、端末装置、通信処理装置、電子交換機、制御装置、または電子計

算機システムなど）である。

〔従来の技術〕

データを秘匿する方法として、暗号がある。暗号法には慣用暗号と公開鍵暗号がある。暗号の鍵には、暗号化用の鍵である暗号化鍵と、復号化用の鍵である復号化鍵がある。慣用暗号は、暗号化鍵と復号化鍵が同一であるか又はその一方から他方を容易に計算できる暗号法を意味する。慣用暗号の暗号アルゴリズムには、ＤＥＳ暗号（"Data Encryption Standard",Federal Information Processing Standards Publication 46, U.S.A., (1977年))、FEAL-8暗号（宮口ほか著："FEAL-8暗号アルゴリズム"、研究実用化報告、第37巻第4/5 号、pp.321-327、NTT(1988年))などがある。公開鍵暗号のアルゴリズムには、ＲＳＡ暗号("R.L.Rivestほか著：A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM,Vol.21, No.2,pp.120-126,(1978年))、Rabin 暗号("M.Rabin 著：Digitalized Signatures and Public-Key Cryptosystems",MIT/LCS/TR-212,Technical Report,MIT(1979年))などがある。

暗号化手段は、任意のデータＡを、鍵Ｙと暗号アルゴリズムにより暗号化して、データＢを出力する変換であり、次式で表す。

Ｂ＝Ｅ（Ｙ，Ａ）

ここで、Ｙの長さは、暗号化鍵の長さである。復号化手段は、データＢを、鍵Ｚと暗号アルゴリズムにより復号化して、データＣを出力する変換であり、次式で表す。

Ｃ＝Ｄ（Ｚ，Ｂ）

ここで、Ｚの長さは、復号化鍵の長さである。ＡとＢの長さは、例えば、暗号文連鎖方式及び／又はパディング（既知のデータによる長さ調整）等の手段を用いることにより、任意の長さでよい。慣用暗号を暗号アルゴリズムとして用いるときは、Ｙ＝Ｚのときに、Ａ＝Ｃとなる。公開鍵暗号を暗号アルゴリズムとして用いるときは、ＹとＺが公開鍵暗号の一対の公開鍵と秘密鍵であるときに、Ａ＝Ｃとなる。

利用者の正当性を認証する方式に、パスワード（又は暗証番号）による方式がある。単一の情報処理装置において、利用者が投入したパスワードを、その情報処理装置で検査する場合、従来は、次のような方式でパスワードの正当性の検証を行っている。

方式１：利用者がパスワードを、情報処理装置に登録する時に、情報処理装置は、パスワードの値をそのまま記憶装置に格納する。次に、情報処理装置は任意の時点で利用者が入力したパスワードを、記憶装置に格納されているパスワードと比較して、一致することにより、利用者の正当性を検証する。

方式２：利用者がパスワードを、情報処理装置に登録する時に、情報処理装置は、パスワードを、情報処理装置が秘密に格納する鍵と、暗号アルゴリズムにより暗号化して記憶装置に格納する。次に、情報処理装置は、任意の時点で利用者がパスワードを入力すると、情報処理装置で秘密に格納する鍵を用いて、記憶装置に格納されているパスワードを、暗号アルゴリズムにより復号化して元のパスワードを出力し、これと利用者が提示したパスワードと一致することにより、利用者の正当性を検証する。

方式３：利用者がパスワードを、情報処理装置に登録する時に、情報処理装置は、パスワードの値を、公開の一方向性関数により変換し、その変換後の値を記憶装置に格納する。次に、任意の時点で利用者が入力したパスワードを、情報処理装置は、一方向性関数により変換し、その変換値が、記憶装置に格納されている値と等しいことにより、パスワードの正当性を検証する。

〔発明が解決しようとする課題〕

方式１の欠点は、記憶装置に格納されているパスワードが情報処理装置の運用者、もしくは他の利用者に盗聴する危険が存在することである。

方式２の欠点は、情報処理装置で秘密に格納する鍵の盗聴により、パスワードが、不正者に盗聴する危険が存在すること、並びに、情報処理装置は、鍵の保管を行わねばならないことである。鍵

は、例えば、記憶装置に保管する。

方式3の欠点は、パスワードを一方向性関数により変換したものは鍵として使用できないため、パスワードの管理と、ファイル又は通信データの暗号化に必要となる鍵の保管とを別に行わねばならないことである。

このように、従来に使用または提案されているパスワード管理方式は、パスワードの安全性に問題があるか、もしくは、パスワードの安全性を向上するための鍵の管理を、パスワードとは別に行わねばならない欠点があった。

この発明の目的は、パスワードを安全に管理し、かつ鍵の管理を容易化したパスワード管理装置を提供することである。

〔課題を解決するための手段〕

請求項1の発明によれば登録用パスワードから鍵が鍵作成手段により作られ、その鍵を用いて第1公開情報が暗号化手段で暗号化されて第2公開情報が作成され、その第2公開情報及び第1公開情報は記憶装置に記憶される。パスワードが入力されるとそのパスワードから鍵作成手段により鍵が作られ、その鍵を用いて第2公開情報が復号化手段で復号化され、その復号化された情報と第1公開情報とが一致するか否か検査され、一致した時は入力されたパスワードが正常であると判定手段で判定される。

請求項2の発明によれば登録用パスワードを鍵として暗号化手段により第1公開情報が暗号化されて第2公開情報が作成され、第1公開情報及び第2公開情報は記憶装置に記憶される。パスワードが入力されると、そのパスワードを鍵として第2公開情報が復号化手段で復号化され、その復号化された情報と第1公開情報とが一致するか否かが判定手段で検査され、一致した時に入力されたパスワードが正常であると判定される。

〔作　用〕

パスワードにより、利用者の正当性を検証することができる。ここで、パスワードは記憶装置には格納しないので、パスワードの安全性が保たれる。また、パスワードを暗号化するための鍵も記憶装置には格納しないので、安全である。

〔実施例〕

情報処理装置1は第1図に示すように、ＣＰＵ2と記憶装置3とが信号線4で接続されており、そのＣＰＵ2と記憶装置3とによりこの発明によるパスワード管理装置が構成される。請求項1の発明では第2図に機能構成を示すように、パスワードから鍵を作成する鍵作成手段11が設けられ、鍵作成手段11はパスワードＰＷを変数とする関数ｆ（ＰＷ）であり、パスワードＰＷのデータが、鍵に十分影響するようにし、かつ鍵が、暗号アルゴリズムに対応した適切な長さとなるようにパスワードＰＷを変換する。以下の実施例では f（・）として慣用暗号を用いる。パスワードＰＷは必要に応じてＰＷ＝ＰＷ1 ∞ＰＷ2 に分解される。∞は2つのデータのそのままの連結を表わし、2ビット以上のデータは複数のデータに分解できる。

登録パスワードＰＷ1 について鍵作成手段11で作られた鍵を用いて、記憶装置3に記憶されている、あらかじめ定めた任意の公開データである、第1公開情報Ｐ1 を暗号化手段12で暗号化して第2公開情報Ｐ2 が作成され、その第2公開情報Ｐ2 は記憶装置3に記憶される。入力されたパスワードＰＷ2 について鍵作成手段11で作られた鍵を用いて、第2公開情報Ｐ2 が復号化手段13で復号化され、その復号化された情報と第1公開情報Ｐ1 とが判定手段14で比較され、正当性が検証される。

第3図にパスワードの登録処理の概要を示す。

ステップ1：

利用者が、登録用のパスワードＰＷ1 を情報処理装置1に入力する。

ステップ2：

情報処理装置1は利用者が入力したパスワードＰＷ1 から、鍵作成手段11により、鍵Ｋ1 を作成する。すなわち、

$$K_1 = f(PW_1) = E(PW_{11}, PW_{12})$$

の処理により、鍵Ｋ1 を生成する。ここで、ＰＷ11 が鍵の長さ未満のときは、あらかじめ定めたビッ

ト値（例えば0）を1つ以上付加して、鍵の長さになるようにする。

ステップ3：

情報処理装置1は、暗号化手段12により鍵K_1で第1公開情報P_1を暗号化して、

$P_2 = E(K_1, P_1)$

とする。

ステップ4：

情報処理装置1は、これを第2公開情報P_2として記憶装置3に格納する。

第4図にパスワードの正当性の検証処理の概要を示す。

前記パスワードの登録処理の後の任意の時点で、パスワードの正当性検証処理が行われる。

ステップ5：

利用者は、情報処理装置1にパスワードPW_2を入力する。

ステップ6：

情報処理装置1は、入力されたパスワードPW_2から鍵作成手段11により、鍵K_2を作成する。すなわち、

$K_2 = I(PW_2)$

$= E(PW_{21}, PW_{22})$ ここで$PW_2 = PW_{21} \| PW_{22}$である、

PW_{21}が鍵の長さ未満のときは、あらかじめ定めたビット値（例えば0）を1つ以上付加して、鍵の長さになるようにする。

ステップ7：

情報処理装置1は、暗号化手段13により鍵K_2で第2公開情報P_2を復号化して、

$P_1 = D(K_2, P_2)$

とする。

ステップ8：

情報処理装置1は、判定手段14により

$P_1 = P_1$

であることを検査し、成立すれば、利用者が入力したパスワードPW_2は正常（すなわち、$PW_2 = PW_1$）であり、成立しなければ、そのパスワードは異常であると出力する。

なお、パスワードの変更と、パスワードの消去は、次のように行う。

パスワードの変更：

利用者は登録済みのパスワードを入力し、その正当性が検証されたときに、新規のパスワードを入力する。情報処理装置1は、利用者が投入した新しいパスワードから鍵作成手段11により鍵を作成し、その鍵で第1公開情報を暗号化して新たな第2公開情報を作成して、その第2公開情報を記憶装置3に格納する。

パスワードの消去：

利用者は登録済みのパスワードを入力し、そのパスワードの正当性が検証されたときに、情報処理装置1は、そのパスワードに対応付けて記憶装置3に登録されている第2公開情報を、記憶装置3から消去する。

パスワードの長さが鍵の長さと同じ時は、パスワードからの鍵作成を省略してパスワードをそのまま鍵として使用することもできる。これは請求項2の発明であり、その機能構成を第5図に第2図と対応する部分に同一符号を付けて示す。つまり登録用のパスワードPW_1が入力されると、暗号化手段12でそのパスワードPW_1を鍵として第1公開情報P_1が暗号化されて、第2公開情報P_2が作成される。検証のためのパスワードPW_2が入力されると、復号化手段13でパスワードPW_2を鍵として第2公開情報P_2が復号化される。その他は第2図の場合と同一である。

〔発明の効果〕

以上述べたようにこの発明のパスワード管理装置によれば、従来のパスワード管理方式に比べて、パスワードは記憶装置には格納されないので、安全である。暗号の鍵を記憶装置に格納する必要がないので、安全である。また、パスワードから作成した鍵を、ファイルや通信データの暗号化のための鍵として用いることもできる。この場合はパスワード管理と暗号化のための鍵管理とが同時に行われて便利である。

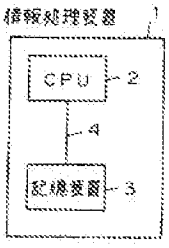
4.図面の簡単な説明

第1図は情報処理装置の構成例を示すブロック図、第2図は請求項1の発明の実施例を示す機能

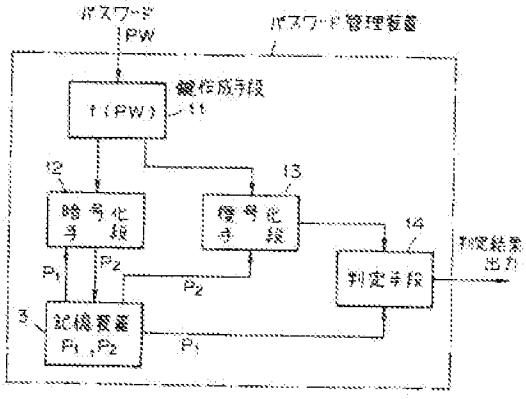
構成図、第3図はこのパスワード管理装置におけるパスワードの登録処理の概要を示す流れ図、第4図は、このパスワード管理装置におけるパスワードの検証処理の概要を示す流れ図、第5図は請求項2の発明の実施例を示す機能構成図である。

特許出願人　日本電信電話株式会社
代理人　弁理士　　草　　野　　卓

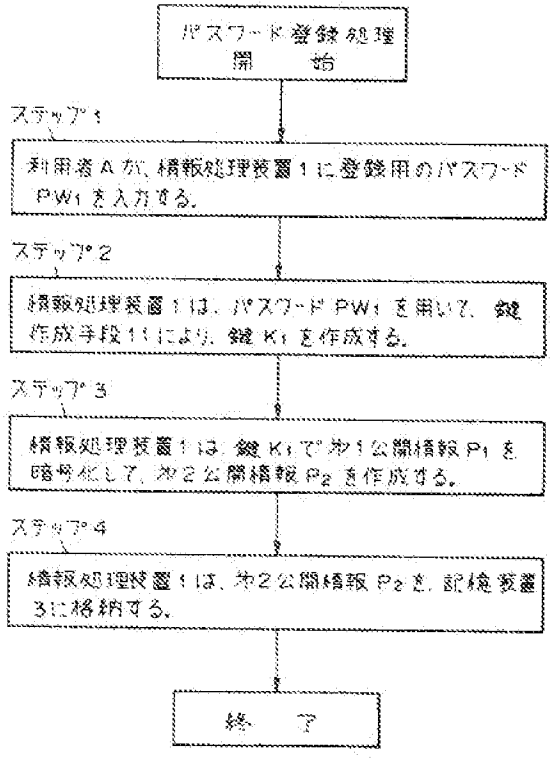
第1図



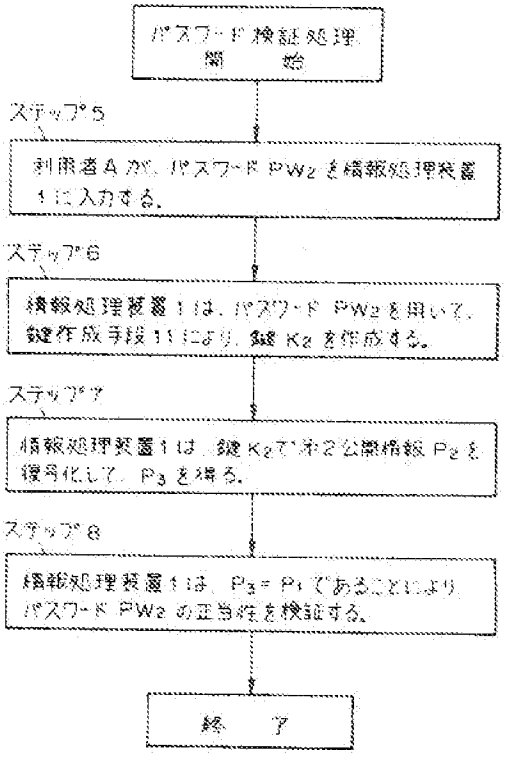
第2図



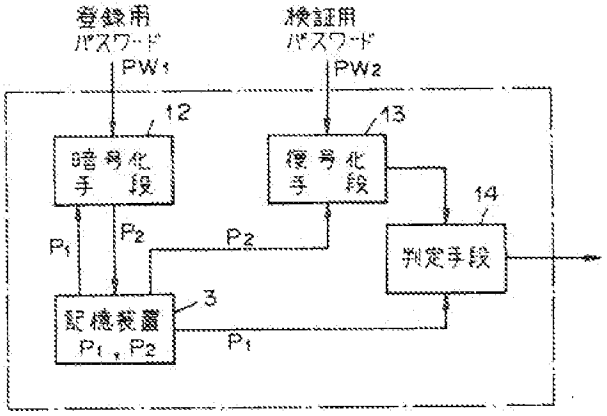
第3図



第4図



第５図


登録用
パスワード
PW1
検証用
パスワード
PW2
12
13
暗号化
手段
復号化
手段
14
判定手段
P1
P2
P2
3
記憶装置
P1，P2
P1